

# TEMA 2: IP MOVIL EN IPv6.

## 1. INTRODUCCION.

Las nuevas mejoras de la tecnología IP móvil actual están pensadas para IPv6.

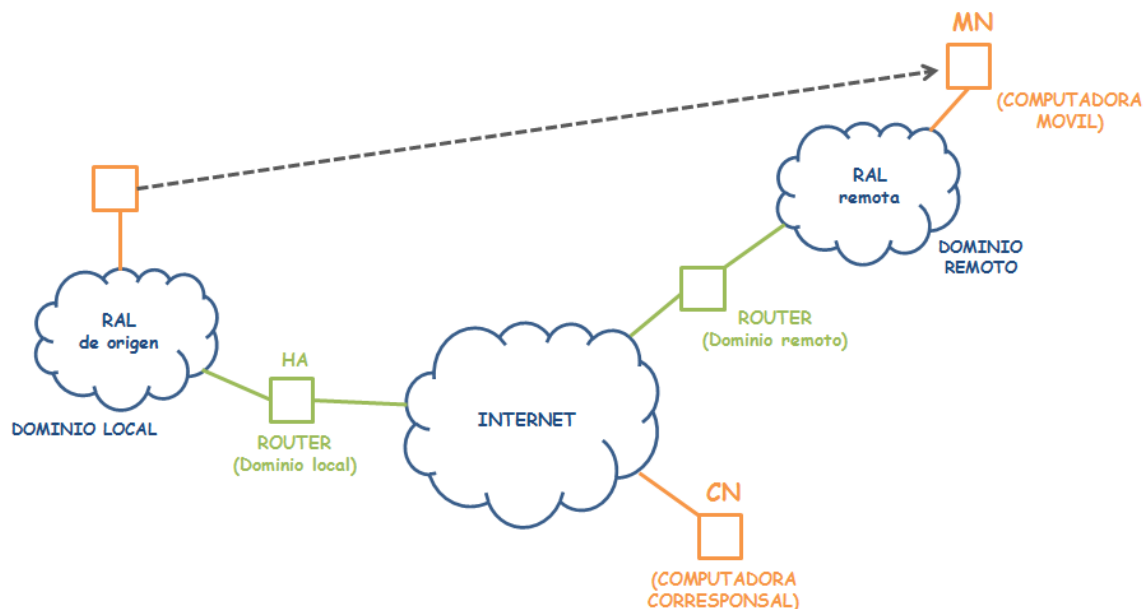
IPv4 móvil es más complejo, debido a que hay mas procesos y los encaminamientos son menos eficientes. IPv4 móvil está obsoleto.

IPv6 móvil es más sencillo y eficiente, ya que hay menos procesos y es más fácil de implantar.

### • OBJETIVOS DE IP MOVIL:

- Los nodos que se mueven de una red a otra tienen que **MANTENER SU DIRECCIÓN IP PERMANENTE** o de origen o nativa y la **CONECTIVIDAD NO DEBE CAMBIAR** en el nivel de red, transporte y aplicación.
- **NADIE DEBE SABER QUE NOS HEMOS MOVIDO**. Se tiene que seguir manteniendo sus comunicaciones (sin cambiar la dirección IP) con independencia de la localización, movimiento e infraestructura de red utilizada.

### • ESCENARIO DE IPV6 MOVIL:



- **NODO MOVIL (MN):** Terminal que se conecta a otra red IP manteniendo su dirección IP.

MN debe poder conservar permanentemente su dirección IP de origen o nativa, independientemente de su ubicación física, y seguir manteniendo sus comunicaciones y recursos como si estuviera en su RAL de origen.

\* **CoA (Dirección Care-of-Address):** Dirección IP temporal de MN en la RAL remota en donde MN esta en un momento dado.

Se utiliza para definir el extremo del túnel. Un túnel consiste en encapsular un paquete IPv6 original en otro paquete IPv6 con la dirección CoA temporal como destino

Un nodo móvil (MN) cuando cambia de red tiene dos direcciones:

1. DIRECCION PERMANETE (Home Address)
2. DIRECCION TEMPORAL DE LA RAL DESTINO (Care-of-Address)

MN envía los paquetes con su CoA. Si pusiera su dirección permanente, el router podría (por seguridad) hacer un filtrado y descartar el paquete porque la dirección de origen no coincide con el prefijo de red (evitando un posible ataque a una maquina por Internet desde una maquina con una dirección extraña)

- **COMPUTADORA CORRESPONSAL (CN):** Terminal que está manteniendo una comunicación con MN. Puede ser cualquier maquina por Internet.  
CN no debe saber si MN se ha movido.  
El nodo correspondal no se da cuenta de que el terminal móvil está en otra red y envía paquetes a la RAL origen de MN.
- **AGENTE DE CASA (HA):** Router con soporte IPmovil en la red original de MN.  
Hace de representante frente a cualquier CN cuando MN no está. Captura paquetes destinados a MN y los reenvía donde realmente se encuentra MN (de forma puntual)  
Los paquetes con destino al MN son interceptados por HA y enviados por un túnel IP móvil a la red remota donde esta MN.  
HA sabe que MN se ha movido, para ello usan mensajes ND (descubrimiento de vecino)
- **INTERACCIONES EN IPv6 MOVIL:** Existen dos posibilidades para enviar un paquete de MN a CN.
  1. **TUNEL BIDIRECCIONAL (TRIANGULO):** CN no sabe nada de MN y se encamina a través de HA.
  2. **ENTREGA DIRECTA:** Optimización del caso anterior.

## 2. PROTOCOLO ND (NEIGHBOR DISCOVERY).

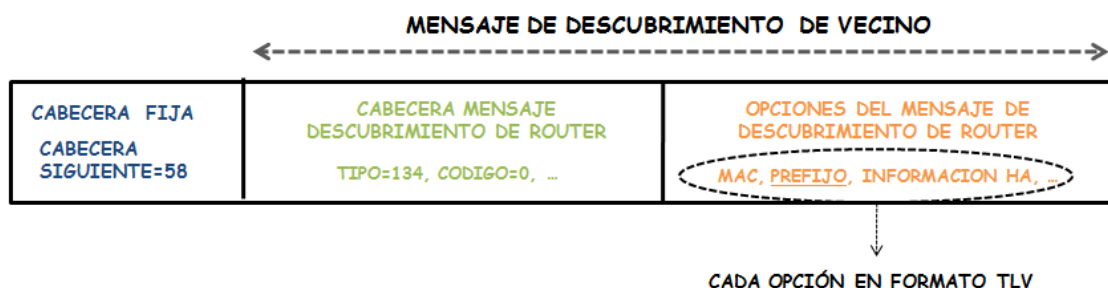
Proporciona la funcionalidad necesaria en red mediante los tipos de mensajes ICMP 133-137. Las funcionalidades son:

1. **AUTOCONFIGURACION DE DIRECCION** (stateless): Asignación automática de una dirección IP a una interfaz de red en función de:
  - \* Prefijo de red recibido del router y en la dirección física (MAC): **EUI-64**
  - \* Prefijo de red recibido del router y en un **NUMERO PSEUDOALEATORIO**.
2. **DESCUBRIMIENTO DE VECINO.** Identificación de las maquinas que están conectadas al mismo enlace.
3. **DESCUBRIMIENTO DE ROUTER Y PREFIJO DE RED.** Para identificar al router y obtener el prefijo de la red.
4. **RESOLUCION DE DIRECCIONES:** Anuncio de un mejor siguiente salto (router) para un determinado destino.

Hay cinco tipos de mensajes ND: Solicitud de router (ICMP 133), Anuncio de router (ICMP 134), Solicitud de vecino (ICMP 135), Anuncio de vecino (ICMP 136) y Redirección (ICMP 137)

### • FORMATO DEL MENSAJE ND DE DESCUBRIMIENTO DE VECINO:

Este mensaje va sobre el mensaje ICMPv6 de anuncio de router.



### 3. ETAPAS DE IPv6 MOVIL PARA ENVIO DE MENSAJES.

- **DESCUBRIMIENTO DE AGENTES:** Proceso de detección de posibles movimientos del MN.

Usa **MENSAJE ND DE DESCUBRIMIENTO DE VECINO**: Transmitido regularmente para indicar su existencia y características mediante un mensaje ICMPv6 de **ANUNCIO DE ROUTER (TIPO=134)** con una o más opciones de información del mensaje ND (dirección MAC, prefijo de red, MTU, información del HA, ...) con información para los MN

Por el prefijo de red, MN sabe si está en la red local o en la remota, para ello comprueba el prefijo del mensaje ND con el prefijo de la red, si coinciden estará en la red local y si no estará en la remota.

- **ADQUISICION DE UNA CoA:** Proceso de obtención de una nueva CoA por MN

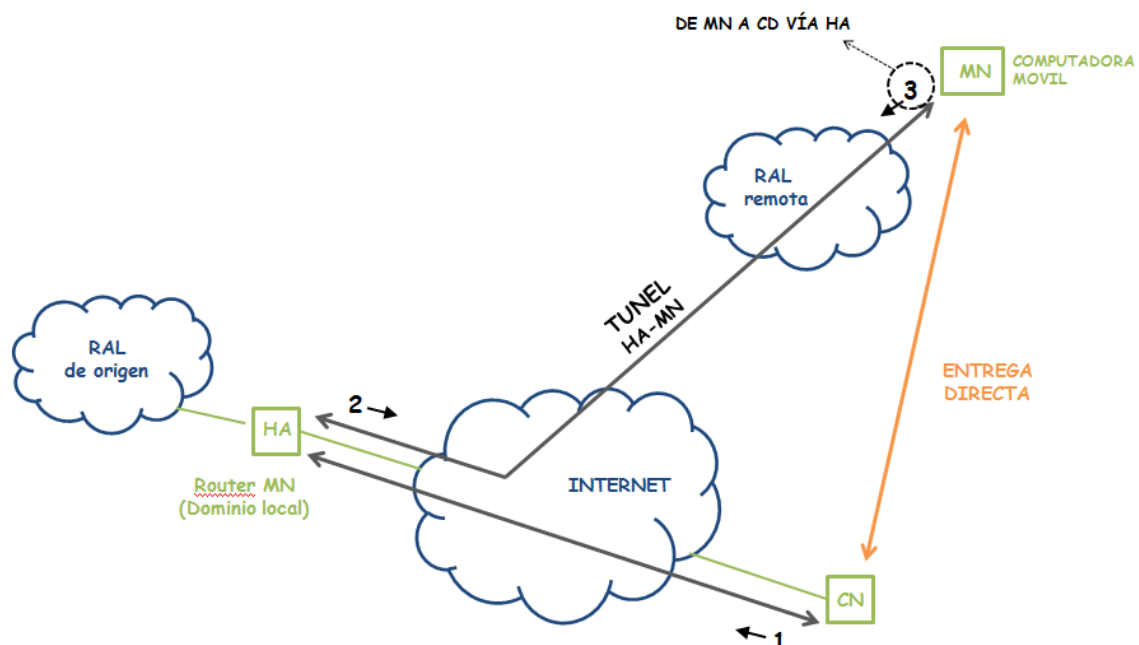
Solo cuando MN detecta que está en una RAL remota obtiene CoA por DHCPv6 o por autoconfiguración (prefijo de red + EUI-64)

- **REGISTRO:** Actualización de la tabla de asociación (binding) del HA.

MN envía a su HA un paquete con la **CABECERA DE EXTENSION DE MOVILIDAD** que contiene la **OPCION DE ACTUALIZACION DE LA ASOCIACION** (BINDING UPDATE) para la actualización de la tabla de asociación de HA (o de un CN)

Una vez que MN obtiene la CoA, añade el prefijo de dirección IPv6 y se registra, es decir, asocia a la dir nativa la nueva dir CoA.

- **ENCAMINAMIENTO Y ENCAPSULADO ("ENTUNELADO"):** Comunicaciones entre MN y uno o varios CN.



1. HA se ocupa de interceptar cualquier paquete destinado a la dirección permanente de MN. Previamente comprueba si el MN está en la RAL de origen mediante un mensaje ND de descubrimiento de vecino creado a través de un **MENSAJE (MULTICAST) ICMPv6 DE SOLICITUD DE VECINO (Tipo 135)**: La respuesta es un **MENSAJE ICMPv6 DE ANUNCIO DE VECINO (Tipo 136)**: que incluye la dirección MAC del vecino.
2. MN pone su **DIRECCION TEMPORAL (CoA) COMO DIRECCION ORIGEN EL PAQUETE** y su **DIRECCION PERMANENTE EN LA CABECERA DE EXTENSION DE OPCIONES PARA EL DESTINO**.  
Permite al MN el uso transparente de CoA a los niveles superiores por encima del soporte MIPv6.

3. **ENCAMINAMIENTO EN TRIANGULO:** Si el MN se comunica con un CN, los paquetes se encaminan desde el CN hacia el HA que los encamina y encapsula al extremo del túnel creado con MN y cuya terminación es CoA.

\* **ENVIO DIRECTO ENTRE CN Y MN (OPTIMIZACION):** MN debe enviar, previamente hacia los CN que se están comunicando con él, paquetes con la cabecera de extensión de Movilidad conteniendo la opción de Actualización de la Asociación (Binding Update).

Mejor que un túnel, CN envía paquetes IPv6 con una cabecera de extensión de Encaminamiento que contiene la dirección IP permanente de MN.

### 3.1. CABECERAS DE EXTENSION EN IPv6 MOVIL.

- **CABECERA DE MOVILIDAD:** Registro de MN con HA y CN (mensajes de asociación)

0	8	16	24	31
CABECERA SIGUIENTE= 59	LONGITUD CABECERA	TIPO DE CABECERA	RESERVADO	
SUMA COMPROBACION		DATOS DEL MENSAJE		

\* **CABECERA SIGUIENTE (8 bits):** El valor 59 identifica que no hay una siguiente cabecera IPv6.

\* **LONG CABECERA MOVILIDAD (8 bits):** Longitud de la cabecera en unidades de 8 octetos (la longitud de la cabecera debe ser múltiplo de 8 octetos, excluyendo los 8 primeros octetos que deben existir como mínimo).

\* **TIPO DE LA CABECERA DE MOVILIDAD (8 bits):** Identifica el correspondiente mensaje de movilidad. Existen 7 tipos:

- **TIPO = 5:** Mensaje de Actualización de la Asociación (Binding Update message) para que un MN notifique de su nueva CoA y dirección IP permanente.
- **TIPO = 6:** Mensaje de Confirmación de la Asociación (Binding Acknowledgment message) que ratifica la recepción de un mensaje tipo=5.

\* **RESERVADO (8 bits):** Uso futuro (todos a cero).

\* **SUMA DE COMPROBACION (16 bits):** Aplicada a toda la cabecera

\* **DATOS DEL MENSAJE (n bits):** Campo longitud variable conteniendo datos opcionales de información.

- **CABECERA DE ENCAMINAMIENTO:** Trafico del MN al CN.

Los paquetes emitidos por MN llevan la dirección origen CoA en la cabecera fija y la dirección permanente de MN en la opción.

0	8	16	24	31
CABECERA SIGUIENTE= 59	LONGITUD CABECERA = 2	TIPO DE ENCAMINAM = 2	Nº ROUTERS = 0	
RESERVADO				
DIRECCION IP PERMANENTE (Home Address)				

\* **CABECERA SIGUIENTE (8 bits):** El valor 59 identifica que no hay una siguiente cabecera IPv6.

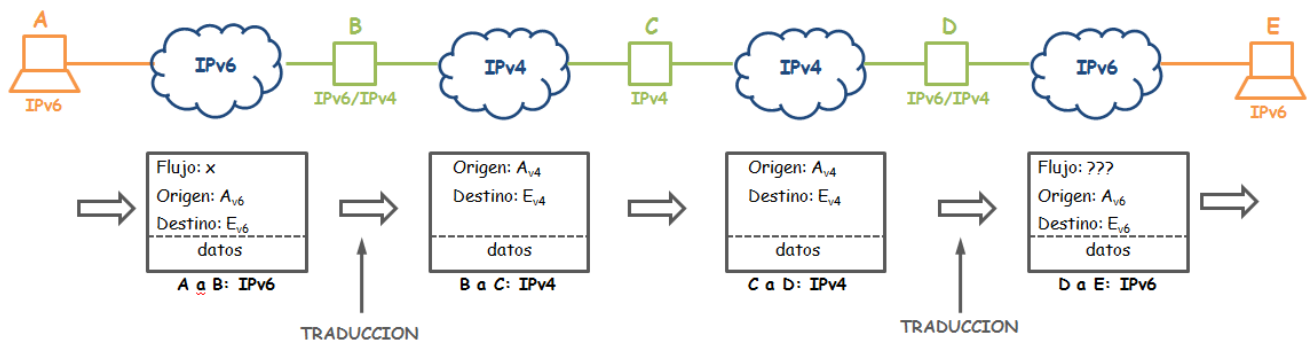
\* **LONG CABECERA MOVILIDAD (8 bits):** El valor 2 identifica la longitud de la cabecera en unidades de 8 octetos, excluyendo los 8 primeros octetos que deben existir como mínimo.

- \* **TIPO DE ENCAMINAMIENTO (8 bits):** El valor 2 identifica la cabecera de enrutamiento usada en MIPv6.
- \* **NUMERO DE ROUTERS (8 bits):** El valor 0 indica que el router debe ignorar la cabecera.
- \* **DIR IP PERMANENTE (124 bits):** La dirección IP permanente (Home Address) de MN.
- \* **RESERVADO (32 bits):** Uso futuro (todo a ceros)

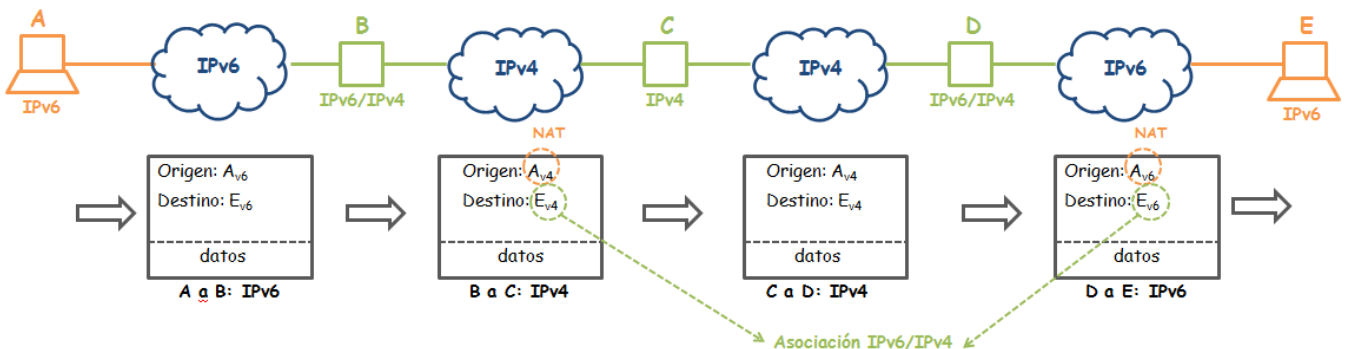
## 4. TRANSICION DE IPv4 A IPv6.

Hasta que se dispongo de routers y servicios IPv6, IPv6 e IPv4 deberán coexistir. Esta coexistencia se puede conseguir mediante distintas técnicas y tecnologías.

### 4.1 TRADUCCION DE INFORMACION DE CONTROL Y DIR. DE RED.

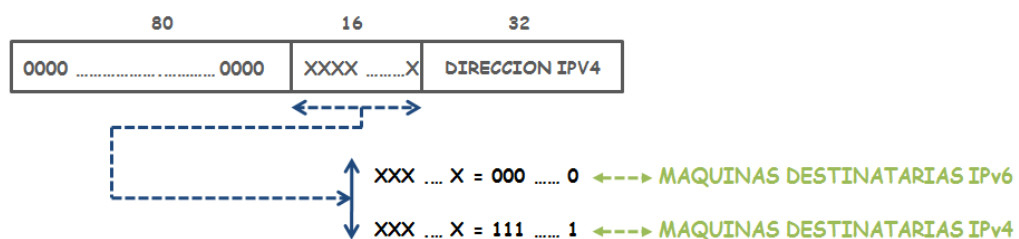


- **SIN FORMATO DE DIR IPv6 COMPATIBLE IPv4:** Vamos a traducir la cabecera IPv6 a IPv4 para poder enviar paquetes por redes IPv4, vamos a traducir los campos que podamos.



Los routers B y D tienen que conocer la asociación Dirección Destino: E<sub>v6</sub> - E<sub>v4</sub> antes de comenzar la transmisión de información entre A y E.

- **DIRECCIONES IPv6 COMPATIBLES IPv4 Y MAPEADAS A IPv4:** Se utilizan direcciones de transición de IPv4 a IPv6, ya que la mayoría de routers son IPv4:



- **MAPEADAS A IPv4 (::FFFF:a.b.c.d):** MAQUINAS DESTINATARIAS IPv4

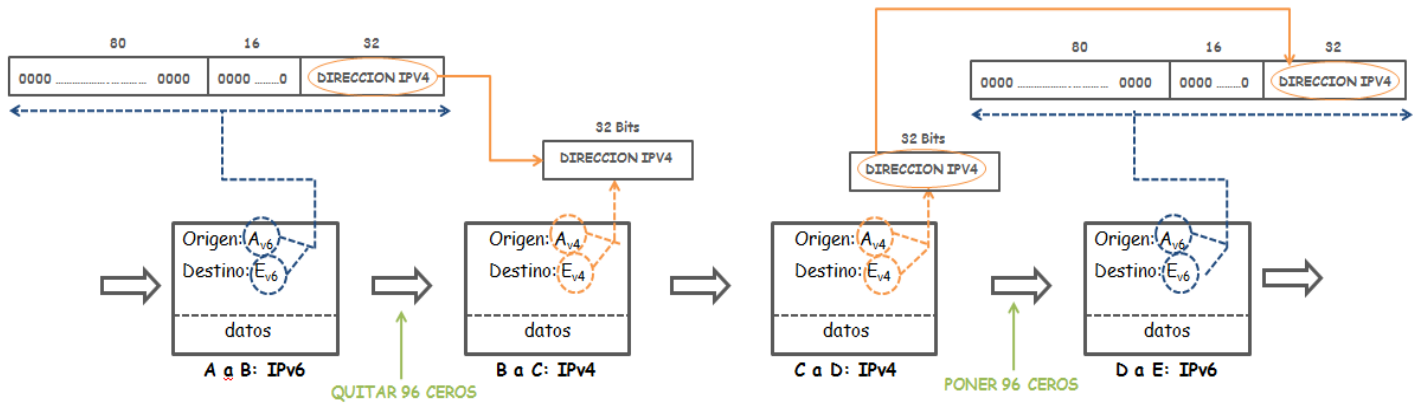
**:: FFFF:IPv4/128**

Se usan para comunicar terminales con doble pila y utilizando direccionamiento IPv6 sobre redes IPv4: Enviar tráfico desde un terminal IPv6 a un terminal IPv4.

- **COMPATIBLES IPv4 (::a.b.c.d):** MAQUINAS DESTINATARIAS IPv6

**::IPv4/128**

Se usan para túneles automáticos sobre IPv4. En este caso B y D no tienen por qué saber nada de las cabeceras, lo único que se hace es poner o quitar 96 ceros.

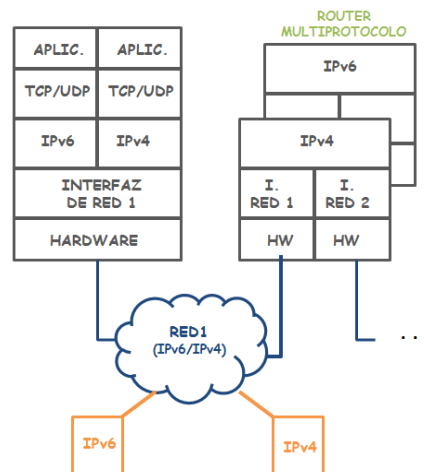


#### • ARQUITECTURAS DE PROTOCOLOS:

Podemos diferenciar dos arquitecturas dependiendo del formato del router que estemos utilizando:

- **UN ROUTER UNA PILA:** Un único router controla los dos protocolos, IPv6 e IPv4, por lo que vamos a necesitar traducir la información de control y de dirección de red.
- **PILA DUAL EN LOS SISTEMAS FINALES:** Funciona en base a una doble pila, con los dos protocolos IPv6 e IPv4 montados sobre el mismo interfaz en el nivel de acceso.

Se envían o reciben paquetes IPv6 o IPv4 indistintamente para el mismo interfaz de la red de acceso. Los datagramas IPv6 irán por la pila IPv6 y los de IPv4 por la pila IPv4.



- \* **ROUTER MULTIPROTOCOLO IPv6/IPv4:** Equivalen a dos routers por separado, aunque en realidad lo que tenemos es un único router con dos pilas de protocolos, una para cada protocolo.

No se necesita ningún tipo de traducción.

Si no se usa un router multiprotocolo deberíamos utilizar en su defecto dos routers independientes uno por cada protocolo.

## 4.2 TUNELES IPv6 SOBRE IPv4.

Los túneles resuelven el problema de la pérdida de información de control de IPv6. Un túnel consiste en encapsular un datagrama IPv6 en un datagrama IPv4.

Si el tamaño del datagrama IPv6 es mayor que el de la red IPv4, la entidad IPv6 lo descartará y mandará a la máquina origen un mensaje ICMPv6 con el tamaño requerido para que el router no necesite fragmentar.

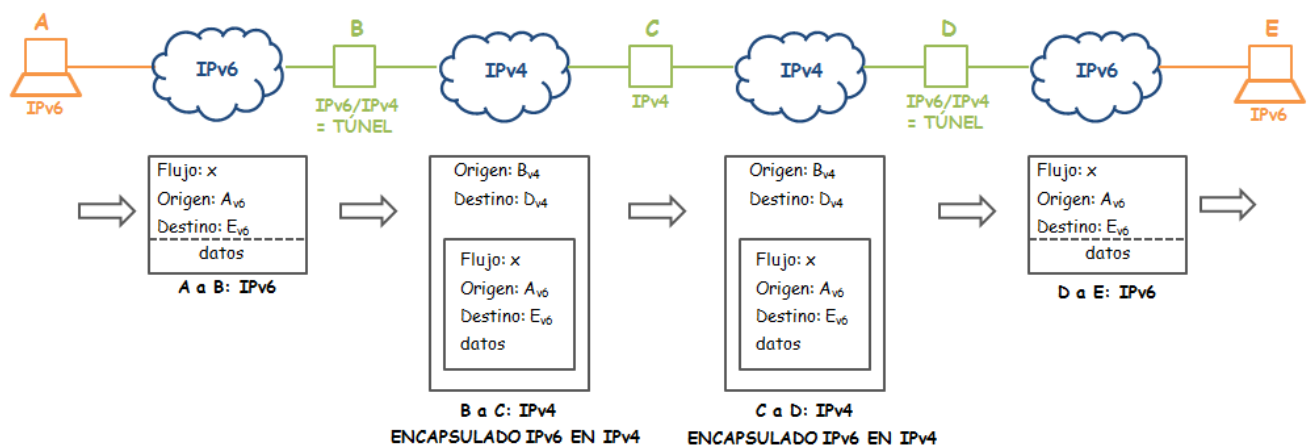
Lógicamente, los datos del datagrama IPv4 son el datagrama completo IPv6. Es necesario insertar 41 (00101001) en el campo protocolo de la primera cabecera de información de control IPv4 que establece el correspondiente túnel.

Los túneles pueden ser: **ROUTER A ROUTER**, **TERMINAL A TERMINAL** o **MIXTO**, es decir, terminal a router o router a terminal.

### • TUNEL CONFIGURADO:

La dirección destino (extremo del túnel) de la cabecera IPv4 que se añade al paquete IPv6 (encapsulación), se tiene que conocer previamente

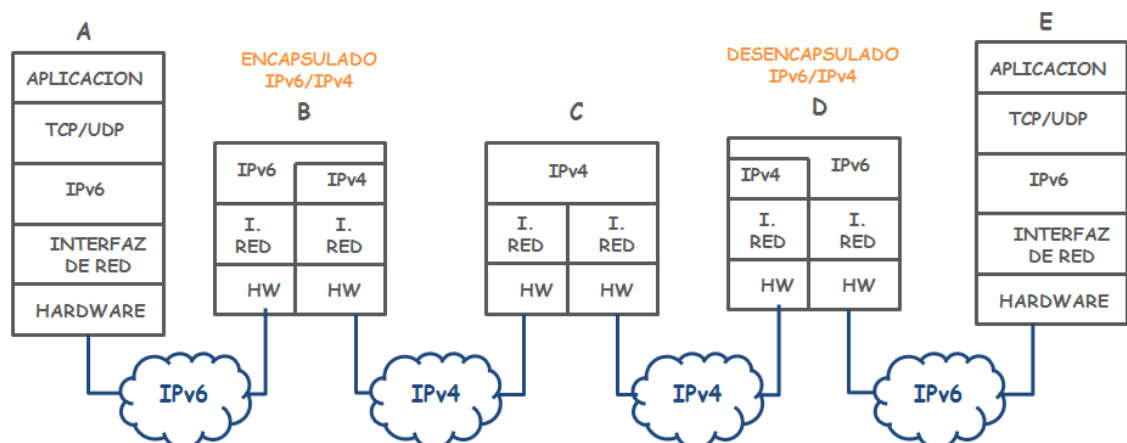
Supongamos un túnel configurado IPv6 sobre IPv4 (B-D) ente A y E.



La entidad IPv4 de B conoce a la par de D, del mismo modo que la entidad IPv4 de D conoce a la par de B. Los extremos del túnel deben conocerse previamente.

**TÚNEL IPv6 SOBRE IPv4 = 2 O MÁS ENTIDADES IPv4 ENTRE LAS 2 ENTIDADES IPv6**  
**LAS DOS ENTIDADES IPv4 MÁS EXTREMAS Y CONTIGUAS A LAS DOS ENTIDADES IPv6 FORMAN EL TÚNEL.**

- **ARQUITECTURA DE PROTOCOLOS:** La arquitectura de protocolos para un túnel configurado consiste en:



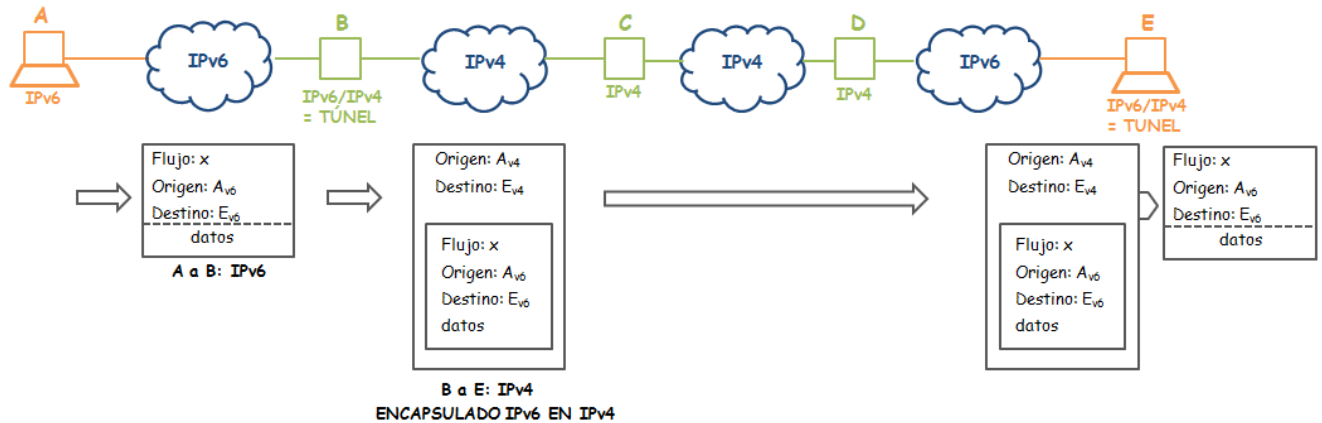


### • TUNEL AUTOMATICO POR DIRECCION IPv6 COMPATIBLE IPv4:

La dirección destino (extremo del túnel) de la cabecera IPv4 que se añade al paquete IPv6 (encapsulación), se obtiene de la dirección destino del paquete IPv6.

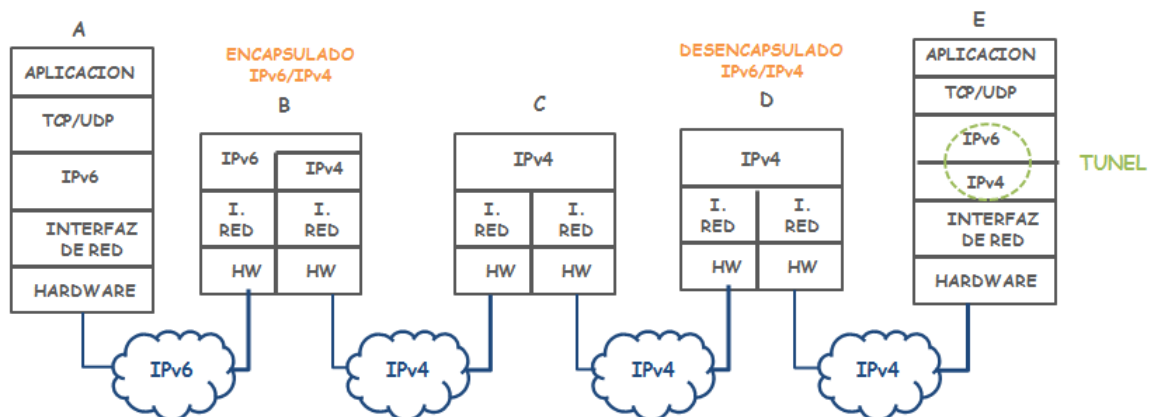
La dirección origen de la cabecera IPv4 que se añade al paquete IPv6 (encapsulación), se obtiene de la dirección origen del paquete IPv6.

Supongamos un túnel automático IPv6 sobre IPv4 (B-E) ente A y E.



**TÚNEL IPv6 SOBRE IPv4 = 2 O MÁS ENTIDADES IPv4 ENTRE LAS 2 ENTIDADES IPv6**  
**LAS DOS ENTIDADES IPv4 MÁS EXTREMAS Y CONTIGUAS A LAS DOS ENTIDADES IPv6 FORMAN EL TÚNEL.**

- **ARQUITECTURA DE PROTOCOLOS:** En este caso la arquitectura de protocolos se diferencia de la anterior en que como en nuestro ejemplo el túnel llega hasta la maquina destino, dentro de ella se dispondrá de un mecanismo de túnel.



### • TUNEL AUTOMATICO 6TO4:

Es una estrategia estandarizada que utiliza una dirección IPv6 (prefijo 2002 en hexadecimal) con la dirección IPv4 "empotrada" en hexadecimal en propia dirección IPv6.

Reemplaza a los túneles automáticos IPv6 sobre IPv4 creados con direcciones IPv6 compatibles IPv4. Actualmente, las direcciones IPv6 compatibles IPv4 se consideran obsoletas y no se implementan ya que no tienen buena escalabilidad (conocimiento previo de la dirección IPv4 del nodo para construir la dirección IPv6).

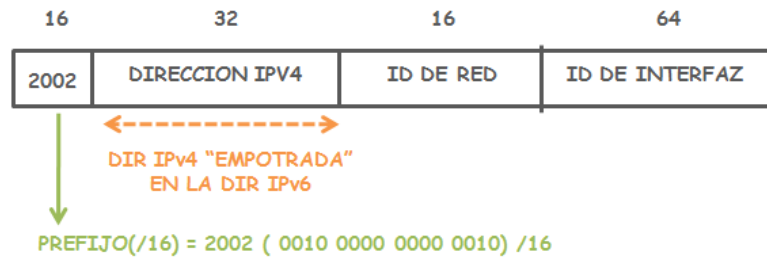
Diseñado para conectar automáticamente, mediante túneles, dominios remotos IPv6 a través de redes IPv4.

El prefijo IPv6 de la dirección de una oficina (/48) se obtiene directamente de la dirección IPv4 del router de dicha oficina. El router de la oficina origen construye el túnel en función de la dirección IPv4 del router de la oficina destino que esta empotrada en la dirección de destino IPv6.



- DIRECCIONES IPv6 DE UNIDIFUSION ESPECIALES DE TRANSICION:

2002:IPv4::/16



Hay que convertir la dirección IPv4 en formato hexadecimal al formato de la dirección IPv6, para poder empotrarla correctamente.